LOG MANAGEMENT

zcrLog

Retain logs.
Keep evidence usable.

zcrLog collects, retains, searches and reports security logs for IT and compliance teams. Evaluate Cloud, Dedicated VM or Hardware Appliance delivery through an approved channel partner.

Deployment options

Cloud / SaaS

Dedicated VM

Hardware Appliance

1 **Collect**

Ingest through supported Syslog UDP/TCP and APIs.

2 **Retain**

Set retention for your package, ingest and available storage.

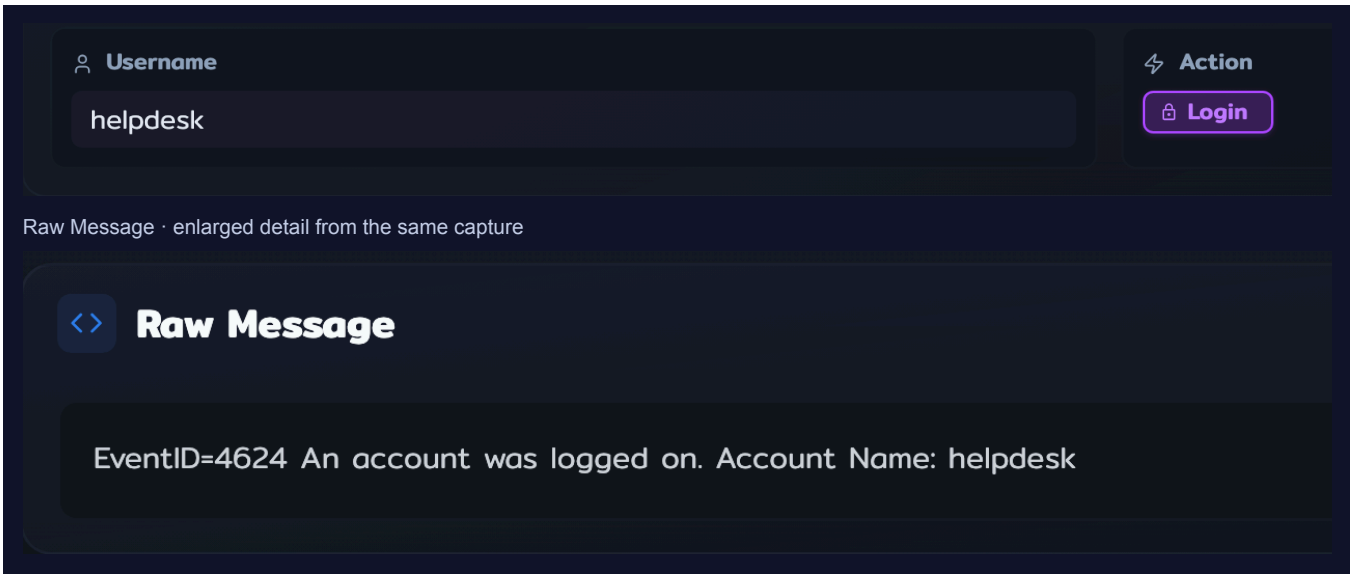
3 **Search and report**

Filter by time, source, user and Event ID.

Conceptual workflow, not a physical deployment architecture.

From an event to usable evidence

DEMO / 4624



Actual demo capture. Events are illustrative, not customer data or measured performance.

Source system: **Windows Server** User: **helpdesk** Action: **Login**

Evaluate log sources and deployment with a partner

Explore the demo ↗ Find a partner ↗

PRODUCT DETAIL

Collection and retention

02

Sizing depends on your log sources, how they send data and how long you must keep it. Dashboard counts show activity; they are not performance benchmarks.

Capability	Scope and qualification
Sources	Firewall, Active Directory, Endpoint Security (for example CrowdStrike Falcon), Microsoft 365, Microsoft Entra ID, AWS CloudTrail, Google Cloud audit logs and Syslog-capable network devices. The parser and API permissions for each source are confirmed in solution design.
Ingest and forwarding	Supported Syslog UDP/TCP and APIs; forward to a Syslog server or log receiver with source, destination and port configuration.
Time reference	Configure NTP and time zones consistently before correlating events from different systems.
Retention	Keeps computer traffic data under Section 26 of the Computer Crime Act for 90 days to 2 years. Actual retention depends on package, ingest and available storage; two years is not included in every tier.
Data integrity	MD5, SHA-1 and SHA-256 integrity checks; AES-128 log encryption.
Archive and export	Archive, JSON/CSV/Parquet export, and incremental or full backup.
Recovery	Restore from archive/backup; monitor disk usage and schedule archive/cleanup according to policy.
Backup destinations	Cloud/SaaS backs up over HTTPS to a cloud service. Hardware Appliance and Dedicated VM can also use external disk, FTP/TFTP or manual download. The destination and its protection are agreed in solution design.
Redundant storage	Available according to the designed architecture. Redundancy is distinct from backup and a tested restore process.

Microsoft 365, Entra ID and cloud sources

zcrLog collects Microsoft Entra ID sign-in and audit logs, and Microsoft 365 workload audit logs (Exchange, SharePoint, Teams) through the Office 365 Management API. It also collects AWS CloudTrail, Google Cloud audit logs and CrowdStrike Falcon logs.

PRODUCT DETAIL

Search and operations

03

Start with an operational question: are logs arriving, when did the event occur, and can the responsible team retrieve the evidence?

Capability	Scope and qualification
Search and filters	Stored logs, filtered by time, source/device, IP, user, event, application, protocol and severity.
Dashboard	Log counts, source Top-N, EPS, storage, retention, recent activity and audit trail in the corresponding console views.
Event context	Incident grouping, MITRE ATT&CK mapping, risk score, attack map and IP intelligence support investigation; they do not guarantee detection of every attack.
Detection rules	Custom, AI-assisted, Sigma and template-based rules. Review and test each rule against your own environment before relying on it.
Reporting	Executive summary reports for a chosen period, with the evidence you select. MDR reports (severity summaries, attack trends, follow-up incidents, technical details and AI recommendations) are delivered as part of the zcrMDR service, not a standalone zcrLog entitlement. zcrSIEM is the separate product for full SIEM operations.
Notifications	Email, Microsoft Teams and LINE through configured detection/alert rules and destination permissions.
Access and audit	Multi-factor authentication (MFA), role-based access control (RBAC), multi-tenant administration; login/logout, access, configuration changes and system errors.
System health	CPU, memory, disk, network, filesystem and service monitoring by deployment. Host-level CPU/RAM/storage thresholds apply to on-premises deployments.

Product features and services

Incident views and reports are product features. Analyst monitoring, incident response and SLAs are services, included only when your agreement names them.

MODEL SELECTION

Hardware Appliance

04

Published specifications for the ICT models. EPS (events per second) values are the published rating for each model. Your partner sizes the model to your workload and confirms the bill of materials before ordering.

Specification	ICT1	ICT2	ICT3
CPU	8 Core	8 Core	16 Core
Memory	16 GB	32 GB	64 GB
SSD	1 TB	2 × 480 GB	2 × 480 GB
HDD	—	2 × 4 TB	2 × 8 TB
Network	1 × 1 GE RJ45	2 × 1 GE RJ45	2 × 1 GE RJ45
Form factor	Mini PC	1 RU	1 RU
Published EPS	1,000	7,000	20,000
Recommended devices	3–5	6–15	16–30
Base retention	90 days[1]	90 days[1]	90 days[1]

Retention

[1] Actual retention depends on ingest and usable storage. Include RAID overhead and reserve space in sizing.

RAID / BOM

RAID 0/1/5/10 is supported by configuration, with RAID 1 as the default on supported models. Confirm the delivered bill of materials with a partner.

Power

Power ratings are not listed in this datasheet. Your partner confirms the electrical requirements and bill of materials of the delivered model before ordering.

What every package includes

Every zcrLog package includes Syslog ingestion, dashboard, MITRE ATT&CK mapping, AI-assisted rules, executive summary, alerts, backup and archive, account security and multi-tenant administration. Onboarding, HA/DR and SLAs are included only when your proposal names them. MDR reports are delivered as part of the zcrMDR service, not a zcrLog package entitlement.

→ **Evaluate log sources and deployment with a partner**

Confirm ingest, retention, usable storage and the bill of materials with your partner before ordering. · Find a partner ↗

MODEL SELECTION

Dedicated VM and Cloud

05

Dedicated VM packages are set by minimum resources and storage; Cloud packages by daily ingest in GB. EPS and device figures are reference values, not interchangeable capacity limits.

Dedicated VM · ICTC

Specification	ICTC1	ICTC2	ICTC3
Minimum CPU	4 vCore	4 vCore	4 vCore
Minimum RAM	4 GB	4 GB	4 GB
Storage	1 TB	2 TB	3 TB
Reference devices	3	5	10
Base retention	90 days	90 days	90 days

Dedicated VM packages do not set an EPS limit; actual throughput depends on the resources allocated to the VM. These values are minimum requirements, and heavier workloads need more resources.

Cloud / SaaS · daily ingest

Package	Cloud1	Cloud2	Cloud3	Cloud4
GB / day	1	3	5	10
Base retention	90 days	90 days	90 days	90 days
Device count	Unlimited	Unlimited	Unlimited	Unlimited

SaaS billing is based on GB/day, without device-count or EPS billing caps. The table shows Cloud1–4; base ingest tiers extend to 50 GB/day. Retention add-ons of 180 days, 365 days and two years are offered only up to 10 GB/day, not for ingest above 10 GB/day.

Product boundary. This document describes zcrLog log retention and evidence workflows, not a complete SIEM or MDR service. zcrSIEM is a separate product and does not require zcrLog.

PRODUCT DETAIL

Partner-led evaluation

06

Your partner works through these points with you during solution design and quotation, so the deployment matches your data and your operating responsibilities.

Evaluation item	What to confirm
Input data	Log sources, protocols, parsers, API permissions, GB/day and peak periods.
Data policy	Retention, residency, access, NTP and archive/backup plan.
Acceptance checks	Verify source events, compare timestamps, retrieve logs, test notifications and perform a restore.
Ownership	Name source, platform and partner owners with an escalation path.
Service scope	Confirm integrations, onboarding, HA/DR, support, SLA and exclusions in writing.

Standards and procurement evidence

Use Thai standard มศอ. 4003.1-2560 as a reference for computer traffic-data retention. Ask the approved partner to match the product certificate to the proposed software version and deployment.

The NECTEC link is the standard itself. For procurement, check the actual certificate, its number, issuer, issue and expiry dates, and the scope applicable to the project.

Using a certified system does not replace your organisation's own responsibilities under the Act.

Read the NECTEC standard ↗ Request evidence through a partner ↗

Plan your evaluation with a zcr partner

Proposals, contracting and customer delivery run through approved distributors, resellers/SIs or MSPs/MSSPs.

Find a partner ↗ Current packages ↗ Open demo page ↗

Specifications and packages may change. Your partner can confirm the current details for your proposal.

7 · Engineering detail and deployment checks

PRODUCT DETAIL

Engineering detail and deployment checks

07

Engineering detail to agree with your partner during solution design. These are design checks, not SLA commitments.

Capability	Scope and qualification
Log forwarding	Log forwarding preserves source data without modification, with source, destination, port, and time-range selection. Check payload completeness and destination timestamps during acceptance testing.
Archive compression	Archive compression can reach up to 15×, depending on log content. Measure the actual ratio on your own logs rather than treating the maximum as a guaranteed storage saving.
Backup and restore	Backup destinations differ by delivery model (see page 2). Include a restore from the chosen destination in acceptance testing.
Storage policy	Schedule archive/cleanup and policy-based deletion at configured usage thresholds. VM storage expansion is subject to the selected package and proposal.
On-premises monitoring	CPU, memory, disk, network, filesystem, and service monitoring at the host level applies to on-premises deployments. These thresholds are not an entitlement guaranteed to every SaaS tenant.
Network thresholds	Network utilization, error-packet, and discard-packet thresholds are available. Validate the monitored interface and available telemetry in your actual environment.
Roles and audit	Additional roles/privileges; login/logout, access records, system-status changes, failures/errors and system structure/configuration changes.
Reports and ingestion	Report ranges: 1, 3, 5, 7, 30, 60 or 90 days, or a custom range. Collection: Syslog UDP/TCP and the Office 365 Management API for Microsoft 365. Connection options: EDR API key and custom integration. Analysis: per-device analytics. The connector for each of your sources is confirmed in solution design.
MSSP and service scope	Multi-tenant administration does not by itself include MSSP resale rights or an MDR service. Entitlements, responsibilities and support scope are set out in your agreement with the partner.